UNITED STATES DISTRICT COURT
DISTRICT OF MAINE

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 622 GRAY ROAD, GORHAM, MAINE 04038	No. 2:25-mj-00080-KFW

AFFIDAVIT IN SUPPORT OF A
SEARCH WARRANT APPLICATION

I, Marshall W. McCamish, being first duly sworn, hereby state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 622 Gray Road, Gorham, Maine 04038, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B. This application seeks authority for a warrant to search for and seize evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(1), (a)(2), and (a)(5)(B), which relate to the knowing transportation, receipt, distribution and possession of child pornography.

2. I am a Task Force Officer ("TFO") with the United States Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI"), and have been since February of 2022. I am presently assigned as a HSI TFO out of the Portland, Maine HSI Office of the Resident Agent in Charge ("RAC"). I also serve as a detective with the Auburn, Maine Police Department ("APD"). I have served as a Law

Enforcement Officer ("LEO") for 21.5 years. As a detective, I have independently and co-investigated a wide range of criminal offenses, such as: Sex Trafficking, Assaults, Robbery, Murder, Elevated Aggravated Assaults, Drug Trafficking, Felony Theft, along with various electronic crimes. As a detective and TFO, I serve as an Internet Crimes Against Children ("ICAC") Investigator. I earned a master's degree in Criminal Justice Administration, along with undergraduate degrees in criminal justice and administration. I am a graduate of the Maine Criminal Justice Academy's Basic Law Enforcement Training Program, located in Vassalboro, ME. In addition, I have completed HSI TFO and Customs Officer Cross-Designation Training. Over the course of my career, I have received specialized training related to criminal investigations as well, specifically related to high technology and cybercrime, child exploitation, and Child Sex Abuse Material (commonly referred to as Child Pornography and as defined in 18 U.S.C. § 2256). Some of the specialized trainings that I have received include: National Computer Forensics Institute ("NCFI") Digital Evidence Investigations, NCFI Vehicle Forensics Course, National White Collar Crime Center ("NW3C") Basic Digital Forensic Analysis: Seizure, NW3C Basic Cyber Investigations: Cellular Records Analysis, NW3C Basic Cyber Investigations: Digital Footprints, NW3C How Computers Work and Store Data, NW3C Introduction to Computer Networks, along with attending multiple digital evidence and investigation seminars through the annual National Cyber Crime Conference. Throughout my law enforcement career, I have independently conducted numerous investigations, written affidavits for the arrest of suspects and for the search of various locations and objects, along with assisting other LEO's with their investigations.

3. This affidavit is intended to provide the facts necessary for a determination of probable cause for the requested search warrant. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

BACKGROUND OF INVESTIGATION

SPECIFIC PROBABLE CAUSE

20. On February 26, 2025, HSI Portland received a lead from HSI Canberra pursuant to an ongoing investigation by the Queensland Police Department (QLD) in Australia. QLD investigators discovered a profile, using the screenname: idontknow12345 on a publicly available photo sharing site, *imgsrc*, that was sharing two albums titled "Nieces feet" and "Nieces feet2". The contents of these folders are publicly available and contain twenty (20) images of a prepubescent child's feet. In some of the photos an adult male's hand(s) is visible. Two of the photos from these publicly available photos contained EXIF and indicate that these photos were taken with a Samsung Galaxy S24 Ultra on two different days: September 5, 2024, and February 13, 2025.

21. On February 17, 2025, QLD investigators identified the individual using the screenname *idontknow12345* also advertised his accounts on two encrypted chat applications, Sessions (on this app the individual using the screenname

idontknow12345 uses the screenname: *dakota*) and Telegram (on this app the individual using the screenname *idontknow12345* uses the screenname: *Kota Q*).

22. The individual using the screenname *idontknow12345*, engaged in messaging with QLD investigators operating in an undercover capacity (UCO). In those chat platforms, user *idontknow12345* discussed his access to children. The individual using the screenname *idontknow12345* stated he had two, 5-year-old, twin nieces and an 8-year-old niece who he does not see very often. The individual using the screenname idontknow12345 posted photographs in his *imgsrc* album as recent as three days prior to uploading. One of the photographs depicts a young girl with the focus on her feet. The young girl appears to be sleeping on the lap of an adult male (UCO believes this adult male to be the individual using the screenname *idontknow12345*).

23. Additionally, the UCO engaged in chat with the individual using the screenname *idontknow12345* on another platform as another person. In that separate chat, the individual using the screenname *idontknow12345* was using the screen name: *Kota Q* and he admitted to committing sexual offenses on all three of his nieces. The individual using the screenname *Kota Q* sent an image showing the naked bottom of his 5-year-old niece (photo_2025-2-11_08-41-53.jpg), whilst an adult male hand can be seen pulling back the panties while the child is sleeping. The individual using the screenname *Kota Q* admitted that he was the person photographed in the image with his niece. The individual using the screenname *Kota Q* has admitted to video-recording some of the abuse using an older phone that he got rid of when he saw someone using his phone.

24. On February 24, 2025, the QLD UCO was engaged in a chat with the individual using the screenname *Kota Q* AKA *idontknow12345*. At approximately 0934

UTC+10 the individual using the screenname *Kota Q* distributed six (6) video files to the QLD UCO. Included in these six (6) videos files were the following:

a. **5yo miss real anal.mp4-** This video is eight minutes and twenty seconds in length and begins with an adult male forcing a prepubescent female, approximately four years old to perform oral sex on him. At approximately two minutes into the video, the adult male carries the prepubescent female onto a bed and forces his penis into her anus. This rape continues for approximately three minutes until the adult male places the prepubescent female on a table and continues to rape her anally. This rape continues for approximately two minutes until the adult male places the prepubescent female on the bed and continues to rape her anally. The video ends at eight minutes and twenty seconds.

b. **1(8)-8.mp4 -** This video is seven minutes and eighteen seconds in length and begins a prepubescent female, approximately five years old, wearing a purple mask. An adult male forces her to perform oral sex on him for approximately one minute and thirty seconds before he begins to rape her vaginally. This rape continues for approximately five minutes until the adult male forces the prepubescent female to perform oral sex on him again. At approximately six minutes and fifty seconds the adult male ejaculates into the prepubescent females' mouth and forces her to swallow it. The video ends at seven minutes and eighteen seconds.

c. **Wertre 2.mov-** This video is seven minutes and fifty-nine seconds in length and begins a prepubescent female, approximately five years old, wearing a purple mask laying on a bed. The adult male forces the prepubescent female

to perform oral sex and then begins to rape her vaginally throughout the video. The video ends at seven minutes and fifty-nine seconds.

25. QLD obtained account information from imgcr regarding the individual using the screenname *idontknow12345*. The following information was obtained:

ACCOUNT INFORMATION

Username: *idontknow12345*

Member since: 2017-09-28

Bio: 05137eaf962d5ca91d2b0062917dcc6bdfd3cdfc a0168a886270c8876039263958 - session @Kotalmno - tg

Email: hidden / Iamkota64@gmail.com

IP logins: 67.246.227.82, 1/6/2024 6:34:08 AM, GMT, +3

67.246.227.82, 1/16/2024 5:06:19 AM, GMT, +3

On February 25, 2025, HSI issued a summons to Charter Communications ("Charter") for subscriber details for the IP addresses: 67.246.227.82, 1/6/2024 6:34:08 AM, GMT +3 and 67.246.227.82, 1/16/2024 5:06:19 AM, GMT +3.

26. On February 26, 2025, Charter provided the following subscriber information pursuant to the summons:

Subscriber

Name: TAMMY SANBORN

Service Address: 622 GRAY RD, GORHAM, ME 040385823

2Account status: Active

27. HSI performed a search of law enforcement databases for the address as well as screenname identifiers in the investigation. HSI discovered that Cody J MERRILL is registered at that address and is a register sex offender in Maine. In September of 2021, Cody Merrill was investigated and criminally charged by the York County Sheriff's Office (21YSO-1214-OF). MERRILL was charged with 1 count of unlawful sexual assault of a minor less than 12 years of age (Class B) and 1 count of unlawful sexual contact (Class D) on October 6, 2024, by the York County Sheriff's Office. MERRILL was subsequently indicted on April 5, 2022. MERRILL ultimately accepted what is known as an Alford plea on January 6, 2023, for count 2 charging unlawful sexual contact (Class D) after which count 1 was dismissed. His sentence was 364 days all, but 15 days suspended, 1 year probation (expired), and is a Tier 1 (10 y.ar) sex offender registrant under Maine Sex Offender Registry laws.

28. On February 25, 2025, HSI Portland agents checked IP address 72.231.251.104 through National Center for Missing and Exploited Children (NCMEC) records and located a previous CyberTip (#136549855) that was submitted by Snap, Inc. which is the internet service provider and parent company that hosts the Snapchat social media platform. The CyberTip identified the user's/suspect's email address as "*iamkota64@gmail.com*." The CyberTip was submitted as a category "B1," which references a minor engaged in a sexual act according to the information provided to NCMEC by Snap, Inc.

29. HSI Portland contacted Gorham Police regarding the residents of 622 Gray Rd. The Gorham Police reported that several adults, to include MERRILL, live at 622 Gray Rd as well as a prepubescent special needs female. Gorham Police also noted

that there are two twin 5-year-old prepubescent female minors related to the residents of 622 Gray Rd.

30. On February 27, 2025, HSI Special Agent Ronald Phillips conducted surveillance at 622 Gray Road Gorham, ME 04038. He observed MERRILL's vehicle ME/Animal Welfare 936AWT parked in the driveway of the residence. At approximately 1510hrs, SA Phillips observed a Gorham School Department van drop of a prepubescent female child at the address, an older unknown male was waiting in the driveway and took the child inside the residence. Gorham PD provided a photograph of a special needs child residing at 622 Gray Rd. When HSI SA Phillips and I reviewed a publicly available social network Facebook page belonging to Tammy Sanborn, we were able to match a photograph that Tammy had posted with the photograph of the special needs girl that Gorham PD had provided us. The social media Facebook page belonging to a Tammy Sanborn did not have privacy setting, so additionally, SA Phillips and I observed additionally photographs posted that depicted Cody MERRILL with multiple children depicted, including what appeared to be the same special needs child that had been observed. Based on this information, it appears that this individual has access to children, so there is a concern that the subject is engaging in hands on offenses with minor children in additional to dissemination of child sexual abuse material.

RELEVANT INFORMATION REGARDING PERSONS INVOLVED IN THE POSSESSION AND DISTRIBUTION OF CHILD PORNOGRAPHY AND ONLINE CHILD ENTICEMENT

31. As set forth above, there is probable cause to believe that an individual at the PREMISES has distributed, transported, received, manufactured or possessed child

pornography. Based upon my training and experience in child sexual exploitation and CSAM investigations as well as through conversations with other officers with knowledge and experience with these types of investigations, your Affiant knows the following:

a. Those who have possessed and/or disseminated CSAM or child sexual exploitation material and/or disseminated obscene material to purported minors have an interest or preference in the sexual activity of children. Persons who are involved with CSAM generally have other sexually explicit materials on additional accounts and/or digital media related to their interest in children, which may consist of photographs, motion pictures, videos, books, slides, text material, computer graphics and digital or other images/visual material for their own sexual gratification. This often includes what may be termed as child erotica or child exploitation material, which may consist of images or videos such as minors in lingerie or text writing involving sex with minors that do not rise to the level of CSAM, but nonetheless fuel their deviant sexual fantasies involving minors. I am aware that this sort of material has been admitted in trials under Fed.R.Evid. 404(b) to prove such things as the possessor's knowledge, intent, motive, and identity to prove the person has a sexual interest in minors. I understand that they may upload or import (meaning transfer) this illicit imagery, including CSAM, onto multiple digital media devices and/or accounts so they can access such material readily to satisfy their prurient desires.

b. Individuals who collect CSAM often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of CSAM and child erotica. They do this to gain status, trust, acceptance, and support and to increase their collection of CSAM and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer (P2P) chat and file sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat (IRC), newsgroups, Internet clubs, and various forms of Instant Messaging such as WhatsApp, Facebook Messenger, Yahoo Messaging, Telegram, and Kik that is sometimes saved on the users' computer or other digital storage media. They may upload files from their CSAM and child erotica collections onto multiple social media accounts where they communicate with others sharing their interests.

c. These individuals typically retain correspondence with these other like-minded individuals. They will make efforts generally to conceal such correspondence as they do with their contraband material, and they often maintain lists of name, account identifiers and other identifying information about individuals with whom they have been in contact and who share the same interests in child pornography.

d. Besides CSAM and child erotica, such individuals often produce and/or collect other written material about sexual activities with minors, which range from fantasy stories to medical, sociological, and psychological

writings, which they save to understand and justify their illicit behavior and desires.

e. Individuals who collect CSAM often collect, read, copy, and/or maintain names, addresses, including e-mail addresses, phone numbers, and lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests, or have CSAM and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or, sometimes, commercial profit. They may maintain these names on computer storage devices, web sites or other Internet addresses. Their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of CSAM as well as identifying the origin of the images or videos to assist with locating the child victims depicted in the imagery.

f. Collectors and distributors of CSAM may also receive sexual gratification, stimulation and satisfaction from contact with children, both in person as well as online, including online UC personas who represent themselves to be minors.

g. Individuals who collect CSAM rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage, their collections of illicit materials. Because of their desire to retain child pornography together with the sense of security afforded by using digital media devices and accounts, the collectors will often retain these CSAM and child exploitation imagery for

lengthy period of time, or even sometimes indefinitely. These individuals usually maintain their collections of sexually explicit materials in the privacy of their own homes and possessions. These individuals may protect their illicit materials from discovery by other through use of passwords, and encryption, and other security measures, including on third party image storage sites via the Internet. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector/manufacture to view and/or access the collection, which is valued highly.

h. In some instances, these depictions are actual photographs or images of the suspect's own sexual activity with past or present child victims. This imagery serves as archives of hands-on offenses and/or CSAM that they enticed real children to produce, which tends to be extremely important to these individuals. Such individuals may keep such depictions as means of plying, broaching or titillating the sexual interests of new or prospective child victims. They may also retain them for lengthy periods of time for their own personal arousal. These offenders are less likely to destroy CSAM or child erotica from child victims known to them. They may send such materials to others with similar deviant interests to brag about their conquests and/or view these produced materials as akin to trophies. In such a manner, hands on offenders may keep child pornography collection to fuel their interests.

COMPUTERS, ELECTRONIC STORAGE AND FORENSIC ANALYSIS

32. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. *Probable cause*. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of

USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or

electronic storage media access, use, and events relating to the crime under investigation.

c. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely

reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

35. *Outbuildings and motor vehicles.* Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable, this includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles.

36. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often

necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The time required for an examination**. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. **Variety of forms of electronic media**. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

37. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

38. Because it appears that multiple people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Dated at Portland, Maine this 27th day of February 2025.

Marshall W. McCamish, TFO
Homeland Security Investigations

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedures

Date: Feb 27 2025

Judge's signature

City and state: Portland, Maine

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title